# Stealth Attacks on Vehicular Wireless Networks

*(Invited Paper)*

Markus Jakobsson*, XiaoFeng Wang* and Susanne Wetzel†
*Indiana University, Computer Science Department, 150 S. Woodlawn Avenue, Bloomington, IN 47405, USA
{markus,xwang}@indiana.edu
†Stevens Institute of Technology, Department of Computer Science, Castle Point on Hudson, Hoboken, NJ 07030, USA
swetzel@stevens.edu

***Abstract*— In this position paper we discuss various issues related to so-called stealth attacks. We elaborate on stealth attacks in the context of three common types of wireless networks, namely ad hoc networks, hybrid networks, and sensor networks. We consider the relevance of these settings to various vehicular environments; e.g., emergency and rescue operations, military operations, and theft recovery. Along with this, we discuss adversarial models. We furthermore explore the level of threat in a set of example situations and discuss potential tools that could be used to reduce the severity of stealth attacks in these contexts.**

## I. Introduction and Related Work

An ad-hoc network is a network formed "on the fly" by a set of participants who typically have not all previously interacted with each other, and may not even have been aware of each other's existence. Ad-hoc networks are highly dynamical and the individual nodes forward traffic on behalf of other nodes. Ad-hoc networks enjoy increasing interest. To a great extent this is due to the fact that ad hoc networks find useful applications in a wide range of situations, including search and rescue operations (e.g., connecting rescue workers at a location with limited availability of cell phone infrastructure), personal area networking (e.g., allowing wireless users to use equipment, such as printers, in public places; and allowing location-based instant messaging), as well as military operations. General ad-hoc networks do neither assume any fixed infrastructure nor the presence of a trusted party.

While ad-hoc networks offer an advanced functionality over traditional networks they at the same time exhibit numerous challenges including the limited wireless transmission range, the broadcast nature of the wireless medium, mobility induced routing changes, and battery constraints of the individual nodes. Perhaps the greatest challenge of all is securing these networks. While this has recently spurred a tremendous amount of research activity (e.g., [11], [15], [17], [3], [4]), these research efforts only consider part of the problem. Some efforts consider how to select and propagate routing information to maximize network performance in the context of cheating or malfunctioning nodes (e.g., [2], [17], [4], [3]). Other efforts consider denial of service attacks on the network (e.g., [8], [16]). None consider these in concert. While it may appear to make sense to study different weaknesses in isolation in general, this is an example of where this is not the case. More particularly, as was shown in [9], the very mechanisms required to defend against all attacks involving propagation of incorrect routing information automatically behooves an attacker attempting to perform a DoS attack, and vice versa. More in general, and as also pointed out in [10], [11], [15], [17], mobile and in particular ad-hoc networking abilities introduce features that end up benefitting attackers as well as honest users.

In this context we discuss in this paper what is refered to as *stealth attacks* [9] with a focus on vehicular wireless networks. Stealth attacks are attacks that can be performed with low effort and cost to and very low risk of detection of the identity (or whereabouts) of the perpetrator. As such these attacks are particularly dangerous since a small number of malicious parties can disconnect a large network with small effort and minimal risk of tracing.

In this paper we elaborate on such attacks in the context of three common types of wireless networks, namely ad hoc networks, hybrid networks, and sensor networks. We then consider the relevance of these settings to various vehicular environments; e.g., emergency and rescue operations, military operations, and theft recovery. Along with this, we describe associated adversarial models. Finally, we explore the level of threat in a set of example situations and discuss potential tools to be used to reduce the severity of stealth attacks in these contexts.

### *Outline*

The remainder of this position paper is organized as follows. In Section II we first briefly review the stealth attack scenario and the kind of attacks introduced in [9]. In Section III we first discuss the difficulty exhibited in theory to secure an ad hoc network against both stealth and DoS type of attacks at the same time. We then briefly focus on some new test results which demonstrate the severity of the problem in practice. In Section we focus on stealth attacks in vehicular wireless environments discussing detailed application scenarios, associated threats and potential countermeasures. We close this paper with some remarks on future work.

## II. Stealth Attacks

Stealth attacks were first introduced in [9]. Stealth attacks are routing attacks which "minimize the cost to and visibility of the attacker but which are about as harmful as brute force attacks". There are two types of stealth attacks, both of which are based on entering false entries or removing valid

entries in the routing tables of honest nodes. The first class of attacks aims to reduce the goodput and isolate victim nodes of the network, or more generally, degrade and partition the network. The second type of attack is geared towards hijacking traffic to and from specific victim nodes in order to allow for malicious actions such as, for example, active eavesdropping and packet filtering. It is important to note that while the possibility of passive eavesdropping is inherent to the broadcast nature of ad hoc networks, the attacker in the second type of attack is outside of the transmission range of the victim, administering the attack from a remote location of the network.

In [9], the attacks are described by means of six different building blocks which in turn are based on the two basic weapons of ”lying” and ”impersonation”: An attacker who is lying, will potentially propagate wrong (routing) information. By means of impersonation, the originating information of correct routing packets is altered.

Combining these weapons (depending on which routing protocol is used – proactive or reactive, with or without maintaining routing caches or tables) – yields the building blocks of ”adding/removing a routing entry with/without impersonation” as well as ”power consumption”. For example, in order to remove an entry using impersonation in case of a proactive routing protocol, an attacker can simply make use of the periodic routing updates. One possibility is for the attacker to announce incorrect routing tables in which entries relating to victim nodes are omitted. Alternatively, in a more sophisticated attack, the malicious node can claim to have the closest route to a victim node thus forcing the other nodes to drop previously announced routes (which they now believe to be longer) to the victim node from their routing tables.

For a detailed discussion on the weapons, building blocks and attacks we refer to [9].

## III. Difficulty to Protect against Stealth Attacks

### A. Critical Tradeoff in Theory

In order to prevent routing attacks in general it has been discussed in literature to introduce the use of strong cryptographic techniques, for example, use authentication methods (e.g., [15], [14] or threshold cryptography (e.g., [17]). However, as was first pointed out in [9], while these solutions will prevent the tampering with routing information and thus thwart routing attacks, they at the same time allow for an attacker to efficiently use a third type of weapon, namely overloading. This is due to the fact that the proposed cryptographic methods are computational expensive and as such allocate a tremendous amount of resources (e.g., battery power). As a consequence, an attacker can easily exploit this fact to attack the system by mounting a DoS type attack injecting invalid messages (e.g., incorrect checksum, wrong encryption, incorrect authentication tag). (It should be noted, however, that overloading may require noticeable active involvement by the attacker, and as such this weapon may potentially not be stealth in nature.)

Since honest nodes cannot a priori distinguish between correct and invalid messages, they will unnecessarily use up their (potentially limited) resources dealing with invalid messages (e.g., trying to decrypt them, checking the authentication tag). Thus, securing a network against both stealth and DoS type attacks at the same time requires delicate balancing of potential countermeasures.

### B. Theory Meets Practice

While the need to balance the tradeoff between preventing stealth attacks and DoS type attacks at the same time is apparent in theory, an important question to answer is how great a need it actually is in practice. Clearly, the answer will have direct impact as to the need of developing effective measures balancing this tradeoff. For example, if securing an ad hoc network against stealth attacks would only amount to a few percent of extra battery draining for a state-of-the art PDA whose battery is expected to last for several hours, this would generally not be considered dramatic. On the other hand, if it would allow for the same battery to be drained in a matter of minutes, the perspective would change completely.

In the following we will briefly outline a test scenario which is being used to assess the importance of balancing the tradeoff between stealth attack and DoS type attacks in practice.

The test scenario depicted in Figure 1 includes three laptop computers, a video camera, and an iPAQ. Two laptop computers and the iPAQ form an ad hoc network, in which the ad hoc routing is done using the AODV routing protocol [13], implemented over 802.11b. While laptop A and the iPAQ as well as laptop B and the iPAQ have an overlapping transmission range, laptops A and B can only communicate with each other through the iPAQ. In order to secure the

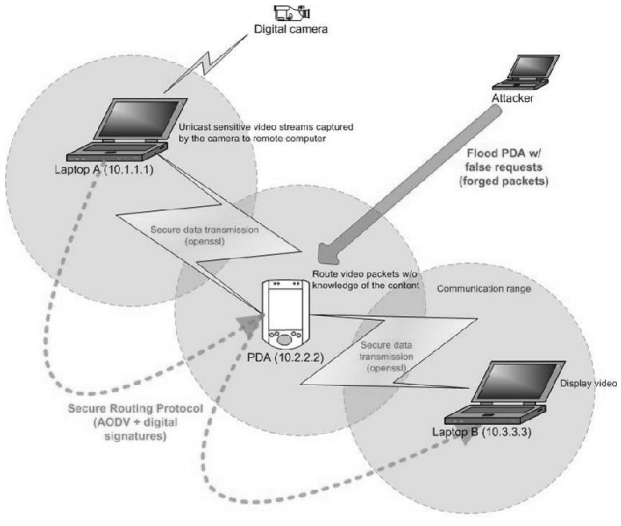


Fig. 1. Battery Draining Attack

routing information in this three node ad hoc network, i.e., provide for authentication, standard crytpographic measures are employed (ElGamal signatures). Furthermore, the traffic from laptop A to laptop B is encrypted, i.e., the iPAQ is transmitting packets without knowledge of the content of the payload.

In standard operation, the battery of the iPAQ is to last for about 6 hours. However, when attacking (as depicted in Figure 1) the ad hoc network by flooding its weakest link, the iPAQ, with an increased number of false requests, i.e., forged packets with invalid signatures, the battery life of the iPAQ is reduced considerably. Preliminary tests have shown that in this setting the battery of the iPAQ can easily be drained in less than 15 minutes. The number of false packets sent through by the third laptop was maximized such that it was not to cause a degrading of the throughput of the video streaming data from laptop A to laptop B. A more detailed discussion of the testing environment and parameters can be found in [6].

## IV. Stealth Attacks and Vehicular Wireless Networks

In this section we focus on three different settings for vehicular wireless networks; ad hoc networks in general, and hybrid respectively sensor networks in particular. We describe their relevance in the context of different applications (e.g., emergency, rescue and military operations) and detail potential threats with a focus on stealth attacks. We furthermore discuss possible measures to thwart the attacks and balance the delicate tradeoff.

### A. Settings and Applications

As pointed out earlier *ad hoc networks* in general are gaining increased interest in various contexts. This is due to their nature of allowing the a network to be established ”on the fly”. In its original definition, an ad hoc network is ”a collection of mobile hosts forming a temporary network without the aid of an established infrastructure or centralized administration” [1].

Of particular interest are *sensor ad hoc* networks which in addition to the usual characteristics of general ad hoc networks exhibit limitations in size, performance and resources (such as battery power, or computational capabilities).

In contrast, *hybrid ad hoc* networks deviate from the original definition in that they allow for inclusion of an infrastructure or centralized administration. Implementations include networks in which the infrastructure or centralized authority is only used before deployment of the network, for example, in order to establish a common secret key amongst all devices that could potentially participate in the ad hoc networking scenario at a later point in time. Alternatively, the devices forming an ad hoc network may occasionally be part of a centralized infrastructure, which in its operation is - to some extent - orthogonal to the intended operation of an ad hoc network. In a third instance a hybrid ad hoc network includes both the ad hoc setting as well as a traditional networking setting at all times. A prominent example is where nodes participate in an ad hoc network but at the same time obtain location information using, for example, a Global Positioning System (GPS) [12].

The large number of potential applications also great contributes to the increased interest in ad hoc networking. This is in particular so in the setting of vehicular wireless networks.

Military operations may benefit from either of the ad hoc settings. For example, a large number of sensors could be dropped from a plane over a hostile environment with the goal to explore the territory of the enemy without having solders invade dangerous areas. Since all of these sensors belong to one specific entity, the sensors may be part of a hybrid type network before deployment. Even after deployment when the sensors operate in ad hoc mode, (some of) these sensors may be able to gather additional information such as GPS location or be equipped to report back by means of a second network to some central authority which is not part of the sensor ad hoc network.

Civilian applications include, for example, emergency operations (search and rescue) as well as location services. Events such as 9/11 have shown the fragility of the traditional static networking infrastructure. At the time it was impossible for emergency and law enforcement personell to communicate with each other not only because traditional networks had been destroyed by the attacks but also because different groups had different backup technologies that could not interoperate with each other. Ad hoc networks can be used to not only bridge the gap between different technologies but also to replace or supplement traditional network infrastructures. For example, by means of an ad hoc network it would be possible for a fire fighter to connect to his colleagues on the floors above and below his location. By extending this chain through all floors in a high-rise building, the fire chief at the control center on the ground floor can be in contact with all his firemen throughout the building at all times.

Everyday applications which are becoming increasingly popular are, for example, applications which allow individuals to obtain location information, driving directions, information on close-by stores, hotels, shopping centers or other points of interest. Furthermore, other so-called telematics applications include automatically initiated road-side assistance, monitoring, surveillance, theft protection as well as recovery. While most of these services to date are operated by means of traditional networking infrastructures (e.g., communication units that connect to a dedicated service center more or less frequently through wireless phone service) the introduction of technologies such as IEEE 802.11 or Bluetooth allow for inter- as well as intra-vehicular communication and thus improve on traditional vehicle-roadside communication. Thus, new applications such as, for example, cooperative driving, collision warning and avoidance become possible. Furthermore, these new ad hoc technologies not only allow extending network functionality and services to areas that are difficult to reach through conventional networks but also provide means for resource sharing which in turn increases the quality of service. For example, during an event in central park which is attended by thousands of people at the time, the local cell phone infrastructure may be overloaded with high probability as too many people may try to use their cell phones at the same time. On the other hand, an ad hoc networking infrastructure among the cell phones could be used to route some of the traffic to adjacent cells outside the park which are less crowded, thus potentially allowing the successful completion of more cell phone calls originated in central park.

### B. Threats

While offering a seemingly unlimited realm of new opportunities, ad hoc networks at the same time exhibit additional risks and threats over traditional networks. As discussed earlier, the most prominent threats in the context of wireless ad hoc networks are routing attacks, in particular those that are stealth in nature. This is particularly so for vehicular ad hoc networks. Depending on the application and the setting, the actual threat, however, may be more or less severe. While military as well as search and rescue settings are most likely to mandate a hybrid networking structure, the employed networks will also include pure sensor networks. Civilian applications, on the other hand, may allow for pure ad hoc networks as well as hybrid or sensor networks.

For ad hoc networks in general, the increased risk is due to the fact that there is no centralized infrastructure or authority that could regulate or secure the networking per se. It is rather the responsibility not only of the individual node or participant to take necessary precautions but also for the nodes as a group to detect and punish misbehavior appropriately. A setting which is totally open has parallels in real life. How can one trust a total stranger in an unknown environment? What is the likelihood that this person will be of help in me getting an intended service? How do I detect misbehavior? How would that be penalized and by whom?

In the case of sensor networks the situation may be even worse, as the individual nodes have limited resources and as such may not be able to gather enough information at the right time in order to make an educated decision and act accordingly.

Hybrid networks, on the other hand, provide support by a central infrastructure or administration. Providing this support before the deployment of the ad hoc network, allows the participating nodes to exchange crucial information in a non-hostile environment. At the same time, however, this limits interoperability and makes the system more difficult to extend. In addition, an attacker may first try to get hold of the inner circle information before launching the acetal stealth attack. In case of continuing support of the ad hoc network by a centralized infrastructure, it is the mere reliance on the authority that will attract increased interest of a potential attacker. A failure or disruption of the centralized service will increase the vulnerability of the ad hoc network.

In addition, hybrid ad hoc networks in emergency or civilian applications may include more than one primary service provider. If their services differ, for example, in reliability, accessibility or price, an attacker may gear his actions towards attacking not only the ad hoc network but also limiting its benefit from the central infrastructure at the same time.

In general, the more limited certain resources are (in particular in sensor networks), the more vulnerable the vehicular network is towards DoS attacks or a combination of the same and stealth attacks. On the other hand, a hybrid vehicular network can make use of alternative channels in order to detect and thwart stealth attacks.

### C. Countermeasures

We propose to use lightweight security primitives and reputation mechanisms to counteract the threat of the stealth attacks in vehicular networks. These approaches help balance prevention mechanisms in the sense that they defend maximally against both DoS attacks and routing attacks.

*1) Lightweight authentication primitives:* It is important to recognize that a large fraction of the attacks against routing protocols take advantage of the existing lack of authentication mechanisms. A second important fact is that battery resources and computational resources typically will be scarce for mobile nodes in most vehicular ad hoc networks, and therefore, that DoS attacks incurring a large amount of computation (meaning expensive, e.g., in terms of battery use) are important to defend against. Thus, authentication mechanisms must be as *light-weight* as possible (i.e., not requiring a substantial computational effort). This clearly encourages the use of symmetric cryptography over the use of asymmetric cryptography, where possible.

While one cannot generally assume that all pairs of nodes in a vehicular ad hoc network share symmetric keys with each other, it is also not generally acceptable to assume that one key is used for larger sets of participants. The latter would not only trivially allow for certain degrees of impersonation but also pose an increased risk in case devices are captured by the attacker. Instead, an interesting approach to study is that of establishing relatively small groups where one and the same symmetric key is used, along with mechanisms to replace this key with pairwise keys if any abuse is detected. Whether this approach proves beneficial or not, it is clear that one needs to either *establish* shared symmetric keys if symmetric keys in any form are to be used during the protocol execution. This is known to be possible using either key exchange or key transport; we will emphasize the latter due to the lowered computational costs for any receiver of a message. This approach blunts computational DoS attacks on the key establishment phase. Alternatively, a hybrid ad hoc setting lends itself for the initial key establishment as well as the continued key updating process.

An alternative to using symmetric key cryptography for authentication is a hash-chain based variant known as TESLA [14]. While this approach is also a possible alternative to standard public key authentication mechanisms[1], it has a potential drawback of large computational requirements when the degree of mobility is high (as reintroduced participants need to compute many hash function steps). Furthermore, TESLA requires a sufficient degree of time synchronization which is also difficult to achieve in high mobility contexts.

While many algorithms can be made light-weight by in-

[1]Traditional public key authentication is likely to be useful for bootstrapping of symmetric key authentication, which is computationally less expensive. It is important to use any public key operations with care to avoid DoS problems. In particular, a key delivery approach might be better suited than key exchange, given the lower costs of initiating the process. By reversing the roles, this can lower the costs for the party contacted by the real initiation. Once a shared key has been established, traditional MAC approaches can be used.

creasing the available storage, this is not a reasonable approach for most settings, and in particular, for most wireless settings. Instead, it is important to develop new tools with reduced requirements, and to use existing ones in a manner that reduces the required effort. Here, the effort is typically shared by two or more participants, and one important consideration may be to achieve a desired balance between these. In particular, it is often desirable that the initiator carries the largest computational burden, in order to reduce the impact of DoS attacks. For example, this could mean using RSA for key transport in a manner in which the initiator requests a key from the contacted node; it could also mean the development of new structures, such as, for example, the hash chain traversal techniques developed for TESLA [5].

*2) Reputation mechanisms:* It is crucial to note that even if one does not consider the negative ramifications of a full-blown authentication structure (namely the cost of performing the cryptographic operations and maintaining the necessary infrastructure), the mere reliance on authentication is not sufficient to thwart stealth attacks. This is so since one must make the assumption that nodes that previously have "well-behaved" later become compromised, and thus, correct authentication of control messages does not correspond to correctness of the control information. This difficulty is enhanced by the fact that it is not common knowledge among the honest servers who exactly is an honest server – whether this set is static or not.

Our proposed technique to deal with the problem, i.e., to detect and discourage misbehavior, is to combine light-weight authentication methods with reputation mechanisms.

In many ad hoc networks, individual nodes can be modeled as self-interested players, trying to maximize their own profits. In this case, reputations can be used to engineer these nodes' incentives, to encourage them to behave honestly. For example, every node treats one's reputation as the priority to relay its messages; as such a node dispersing false routing information could be penalized by making it difficulty for him to dispatch its own messages. With a proper design of reputation mechanism, some equilibrium could be achieved in which every node only distributes the routing information from reliable sources. Therefore, even in the presence of the nodes being compromised by adversaries, the reliability of the system could still be assured as long as these nodes do not take over large portion of an ad hoc network.

However, several problems need to be solved when deploying reputation mechanisms in ad hoc networks. First, the distribution of every node's reputation could be slow and costly. Second, attacks on the reputation mechanism itself may occur. For example, a malicious node may deliberately frame an honest node. In hybrid networks, however, these problems could be mitigated by means of the inherent central infrastructure as it allows the use of a hybrid reputation mechanism, integrating local reputation information with global information thus improving on methods that rely exclusively on local or centrally administered information. Moreover, using globally available reputation information allows the use of collaborative methods [7] to counteract attacks on the reputation mechanism. In order to reduce costs as well as the dependency on connectivity nodes should connect to the central only periodically.

Potential solutions for vehicular sensor networks must account for the limited (computational) resources. Since nodes are either cooperative (working properly) or malicious (being compromised by adversaries), reputation in this context could be used to describe a node's reliability, i.e., how frequently the node behaves improperly. In order to make it difficult for an adversary to predict other nodes' behavior, a node may randomize its strategy (trust or distrust) w.r.t. another node according to its reputation.

## V. Conclusion

In this position paper we have proposed some approaches to address the difficult issue of finding a tradeoff that allows to balance the risk of stealth and DoS attacks in vehicular ad hoc networks. In future work, the viability of these approaches will be verified, and the solutions will be detailed and extended.

## Acknowledgments

The authors would like to thank Nicolas Girard and Charles-Henri De Boysson for their valuable comments and input.

## References

[1] J. Broch, D. B. Johnson, and D. A. Maltz. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks. *Internet Draft, draft-ietf-manet-dsr-03.txt*, 1999.

[2] S. Buchegger and J.Y. Le Boudec. Performance Analysis of the CONFIDANT Protocol: Cooperation Of Nodes— Fairness In Dynamic Ad Hoc NeTworks. *Proceedings of IEEE/ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*, 2002.

[3] S. Capkun, J. P. Hubaux, and L. Buttyan. Mobility Helps Security in Ad Hoc Networks. *Proceedings of MobiHoc*, 2003.

[4] S. Capkun, L. Buttyan, and J. P. Hubaux. Self-Organized Public-Key Management for Mobile Ad Hoc Networks. *IEEE Transactions on Mobile Computing, Vol. 2, Nr. 1*, 2003.

[5] D. Coppersmith and M. Jakobsson. Almost Optimal Hash Sequence Traversal. Financial Cryptography '02. Also available at http://www.markus-jakobsson.com

[6] C.H. De Boysson, N. Girard, and S. Wetzel. Assessing the Risk of Battery Draining in Ad Hoc Networks. *In Preparation*, 2004.

[7] C. Dellarocas. Immunizing Online Reputation Reporting Systems Against Unfair Ratings and Discriminatory Behavior. *Proceedings of ACM Conference on Electronic Commerce*, 2000.

[8] M. Jakobsson and F. Menczer. Untraceable Email Cluster Bombs: On Agent-Based Distributed Denial of Service. http://www.markus-jakobsson.com, 2003.

[9] M. Jakobsson, S. Wetzel, and B. Yener. Stealth Attacks on Ad Hoc Wireless Networks. *Proceedings of IEEE VTC 2003-Fall*, 2003.

[10] V. Kärpijoki. Signalling and Routing Security in Mobile and Ad Hoc Networks. http://www.hut.fi/~vkarpijo/iwork00/, 2000.

[11] J. Lundberg. Routing Security in Ad Hoc Networks. http://www.tml.hut.fi/~jlu, 2000.

[12] M. Mauve and J. Widmer. A Survey on Position-Based Routing in Mobile Ad Hoc Networks. IEEE Network, 2001.

[13] C. E. Perkins and E. M. Royer. Ad Hoc On-Demand Distance Vector Routing. *Proceedings of IEEE Workshop on Mobile Computing Systems and Applications*, 1999.

[14] A. Perrig, R. Canetti, J.D. Tygar, and D. Song. The TESLA Broadcast Authentication Protocol. *RSA CryptoBytes* http://www.rsasecurity.com/rsalabs/cryptobytes/ , 2002.

[15] F. Stajano and R. Anderson. The Resurrecting Duckling: Security Issues for Ad Hoc Wireless Networks. *Proceedings of International Workshop on Security Protocols*, 1999.

[16] X. WANG AND M.K. REITER. Defending Against Denial-of-Service Attacks with Puzzle Auctions. *Proceedings of IEEE Symposium on Security and Privacy*, 2003.
[17] L. ZHOU AND Z. J. HAAS. Securing Ad Hoc Networks. http://www.ee.cornell.edu/~haas/Publications/network99.ps, 1999.